Groups Generated by n Operators Each of Which is the Product of the $n-1$ Remaining Ones.

BY G. A. MILLER.

The case when $n=3$ has recently been considered.* When $n=2$ the groups are evidently cyclic and hence require no consideration in this connection. In the present paper we shall consider $n>3$, and we shall first assume that the products of the $n-1$ operators are independent of their orders and hence all of them must be commutative. Representing the n operators under consideration by $s_1, s_2, \ldots, s_n$ we have by hypothesis, s_n being any one of the n operators, that

$$s_1 s_2 \ldots s_{n-1} = s_n, \text{ or } s_1 s_2 \ldots s_n^{-1} = 1.$$

From the two equations

$$s_1 s_2 \ldots s_{n-1} = s_n \text{ and } s_1 s_2 \ldots s_{n-2} s_n = s_{n-1}$$

it follows, by multiplying one into the inverse of the other, that *any two of these n operators have the same square* and, by direct multiplication, that *the* $2(n-2)^{\text{th}}$ *power of each operator is the identity.*

If we substitute for $s_1, s_2, \ldots, s_{n-1}$ the $n-1$ independent transpositions $a_1 b_1, a_2 b_2, \ldots, a_{n-1} b_{n-1}$, there results a system of operators which satisfy the given conditions for every value of $n>3$. These n operators clearly generate the Abelian group of order 2^{n-1} and of type $(1, 1, 1, \ldots)$. From the given theorem it results that this is the only system of Abelian groups of type $(1, 1, 1, \ldots)$ which may be generated by n operators satisfying the given condition, if we exclude the trivial case when the group is cyclic. By letting $s_1 = s_2 = \ldots = s_n$ it is clear that the cyclic group of order $n-2$ might be said to be generated by operators satisfying the given condition. To avoid the consideration of such trivial cases we shall assume that no two of the n operators under consideration are identical. From this assumption and the given theorem it follows that no more than one of them can be of odd order, and if the order of one of them is an odd number the order of the others is twice this odd number.

* Bulletin of the American Mathematical Society, vol. 13 (1907), p. 381.

Hence the theorem: *If the order of one of the n operators $s_1, s_2, \ldots, s_n$ is divisible by 4, all of them have the same order. If this condition is not satisfied, either all of them have for their order the double of the same odd number or $n-1$ of them have this order while the remaining one has the odd number for its order.*

As the operators $s_1, s_2, \ldots, s_n$ have a common square and are commutative, we have the equations $s_\alpha^2 = s_\beta^2$, $s_\alpha s_\beta^{-1} = s_\alpha^{-1} s_\beta$, $(s_\alpha s_\beta^{-1})^2 = s_\alpha s_\beta^{-1} s_\alpha s_\beta s_\beta^{-2} = 1$. That is, each of these operators may be obtained by multiplying any other one by some operator of order 2. Hence all of them may be obtained by multiplying one by the identity and different operators of order 2. On the other hand, it may be observed that if $t_1^2 = t_2^2$ and if $t_1 = \rho t_2$, where $\rho^2 = 1$, it is necessary that $t_1 t_2 = t_2 t_1$. For, as the second equation near the beginning of this paragraph does not imply that $s_\alpha s_\beta = s_\beta s_\alpha$ it follows that $t_1 t_2^{-1} = t_1^{-1} t_2$, or $\rho = t_1^{-1} t_2$. Hence $t_1^{-1} t_2 t_1^{-1} t_2^{-1} t_2^2 = t_1^{-1} t_2 t_1^{-1} t_2^{-1} t_1^2 = t_1 t_2 t_1^{-1} t_2^{-1} = 1$. From this it results that the commutator of t_1, t_2 is the identity and hence these operators are commutative. We have thus arrived at the theorem: *The necessary and sufficient condition that two different operators which have a common square are commutative is that one is the product of the other into an operator of order* 2.

From the preceding paragraph it follows that the n operators under consideration may be represented as follows: $s_1, \rho_1 s_1, \rho_2 s_1, \ldots, \rho_{n-1} s_1$; where $\rho_1, \rho_2, \ldots, \rho_{n-1}$ represent $n-1$ different operators of order 2 which are commutative with each other and with s_1. Since

$$s_1 = \rho_1 s_1 \cdot \rho_2 s_1 \cdots \rho_{n-1} s_1 = \rho_1 \rho_2 \cdots \rho_{n-1} \cdot s_1^{n-1}$$

and $s_1^{2(n-2)} = 1$, it results that $\rho_1 \rho_2 \cdots \rho_{n-1} = s_1^{n-2}$. The n commutative operators $s_1^{n-2}, \rho_1, \rho_2, \ldots, \rho_{n-1}$ must therefore have the property that each of them is equal to the product of all the others. When $s_1^{n-2} = 1$ the $n-1$ operators $\rho_1, \rho_2, \cdots \rho_{n-1}$ have the same property. As the group generated by $s_1, s_2, \ldots, s_n$ is identical with the one generated by $s_1, \rho_1, \rho_2, \ldots, \rho_{n-1}$, we have the interesting theorem: *If a group G is generated by n commutative operators such that each is the product of all the others, then G is the direct product of a cyclic group whose order divides* $2(n-2)$ *and an Abelian group of order* 2^a *and of type* $(1, 1, 1, \ldots)$. Moreover, any such direct product may be generated by n operators which satisfy the given condition.

While $n-2$ of the operators $\rho_1, \rho_2, \ldots, \rho_{n-1}$ can always be replaced by independent transpositions, as was observed in the second paragraph, it may be possible to replace them by operators which generate a much smaller group. For instance, when $n = 2^\beta$ and $s_1^{n-2} = 1$, it is possible to replace all of them by

the operators of order 2 in the Abelian group of order 2^β and of type $(1, 1, 1, \ldots.)$. If $s_1^{n-2} \neq 1$ and $n = 2^\beta - 1$, they may be replaced by $n-1$ of the operators of the same Abelian group, while s_1 may be so chosen that its $(n-2)^{\text{th}}$ power is equal to the remaining operator of order 2. In each of these cases the order of G is either 2^β or $2^{\beta-1}$ into the order of s_1.

Non-Abelian Groups.

When the n operators $s_1, s_2, \ldots., s_n$ are not supposed to be commutative, it is generally possible to select them in such a way as to satisfy the condition expressed in the heading of this article and to generate any one of a large number of different types of groups. This is especially true when $n > 4$, as will appear in what follows. It is, however, possible to establish a few general theorems of interest, and to exhibit many fundamental properties of the possible groups when $n = 4$, by means of elementary considerations. One of these theorems may be stated as follows: *If the n operators $s_1, s_2, \ldots., s_n$ are arranged cyclically and the product of any $n-1$, in order, is equal to the remaining one, then all of them have a common square.*

The proof of this theorem follows almost directly from the defining equations; for the two equations

$$s_1 s_2 \ldots. s_{n-1} = s_n, \quad s_2 s_3 \ldots. s_n = s_1$$

imply $s_1^{-1} s_n = s_1 s_n^{-1}$ and hence $s_n^2 = s_1^2$. Similarly we may prove that $s_1^2 = s_2^2$, etc. Moreover, it results that

$$s_{n-1} s_{n-2} \ldots. s_2 s_1 = (s_1 s_2 \ldots. s_{n-1})^{-1} \cdot s_1^{2(n-1)} = s_1^{2(n-2)} s_n,$$

and this includes a second proof of the fact that the $2(n-2)^{\text{th}}$ power of each operator is the identity whenever the n operators are commutative.

If $s_1, s_2, \ldots., s_n$ are any n different operators of order 2 which satisfy the condition

$$s_1 s_2 \ldots. s_n = 1 \qquad (A)$$

it follows that $s_{\alpha+1} \ldots. s_n s_1 s_2 \ldots. s_{\alpha-1} = s_\alpha$; $\alpha = 1, 2, \ldots., n$. That is, the product of any $n-1$ of them in order is the remaining one. Of $n \geqq 5$ the operators of (A) may be so chosen as to generate any symmetric group whose degree exceeds a given number $(m-1)$. To prove this statement it is only necessary to observe that s_1, s_2 may be so selected as to generate the dihedral group of order $2p$, $m \geqq p > \frac{m}{2}$ and p being prime, according to the well-known theorem due to Tchébycheff. Hence it is possible to choose the three operators (s_1, s_2, s_3)

of order 2 so that they generate a transitive group of degree m involving negative substitutions. This must be the symmetric group, since it involves the cycle of order p and such a cycle cannot occur in any non-symmetric and non-alternating primitive group unless its degree is p, $p+1$, or $p+2$.* If m had one of the last three values it would be easy to select s_1, s_2, s_3 so that the primitive group generated by them would involve a transposition. This completes the proof of the statement in question, since it is only necessary to find an operator of order 2 which transforms $s_1 s_2 s_3$ into its inverse in order to find the five operators of order 2 such that $s_1 s_2 s_3 s_4 s_5 = 1$.

From the preceding paragraph it is clear that the number of different types of groups that may be generated by $s_1, s_2, \ldots, s_n$ $(n > 4)$ is so large as to make it questionable whether it is desirable to endeavor to give an enumeration of all the possible types. When $n = 4$ the matter becomes comparatively simple, and hence we restrict ourselves to this case in what follows. From the equations

$$s_1 s_2 s_3 = s_4, \quad s_2 s_3 s_4 = s_1, \quad s_3 s_4 s_1 = s_2, \quad s_4 s_1 s_2 = s_3$$

we obtain

$$s_1 s_2 s_3 s_4^{-1} = s_1^{-1} s_2 s_3 s_4 = s_1 s_2^{-1} s_3 s_4 = s_1 s_2 s_3^{-1} s_4 = 1.$$

Since s_3, s_4 transform $s_3 s_4^{-1}$ into its inverse,† they must also transform $s_1 s_2$ into its inverse. That is, the product of any two of these operators, taken in cyclical order, is transformed into its inverse by each of the other two. We shall now consider the group (H) generated by the two operators

$$s_1 s_2^{-1}, \quad s_2 s_3^{-1}.$$

Each of these operators is transformed into its inverse by s_2, and s_3^{-1} transforms $s_2 s_1^{-1} = s_2^{-1} s_1^{-1} \cdot s_2^2$ into $s_1 s_2 \cdot s_2^2 = s_1 s_2^{-1} \cdot s_2^4$. That is, $s_2 s_3^{-1}$ transforms $s_1 s_2^{-1}$ into $s_1 s_2^{-1} \cdot s_2^4$. Since s_2^4 is invariant, it follows that $\{s_1 s_2^{-1}, s_2 s_3^{-1}\}$ is metabelian and its commutator subgroup is the cyclic group generated by s_2^4. When the common order of s_1, s_2, s_3, s_4 is either 2 or 4, $\{s_1 s_2^{-1}, s_2 s_3^{-1}\} = H$ is Abelian and the group G generated by s_1, s_2, s_3, s_4 may be obtained by extending H by means of an operator of order 2 or 4 which transforms each operator of H into its inverse. In this case H is either cyclic or the direct product of two cyclic groups.

When H is cyclic G may be any dihedral group whose order exceeds 6, since any such group is generated by four operators of order 2 which satisfy the condition (A). In fact, the two remaining dihedral groups can be generated by

* Bulletin of the American Mathematical Society, vol. 4 (1898), p. 140.

† Archiv der Mathematik und Physik, vol. 9 (1905), p. 7.

four operators satisfying (A) if it is not implied that all the operators are distinct and that none of them is the identity. Hence the theorem: *Every dihedral group may be generated by four operators, each of which is a product of the other three.* When the order of this dihedral group exceeds 6, it may be assumed that the four operators are distinct. By dimidiating* any two dihedral groups with respect to the cyclic subgroups of half their orders we obtain a group G which may be generated by four operators of order 2, each of which is a product of the other three. If s_1', s_2' and s_1'', s_2'' respectively are generators of the dihedral groups in question, each of these operators being of order 2, the four generators of G $s_1' s_1''$, $s_1' s_2''$, $s_2' s_2''$, $s_2' s_1''$ clearly satisfy the conditions imposed on s_1, s_2, s_3, s_4. Hence it follows that *every group which may be obtained by extending the direct product of two cyclic groups by means of an operator of order 2 which transforms each operator of this direct product into its inverse may be generated by four operators of order 2, each of which is a product of the other three.*

When H is an Abelian group of even order, it is well known that we can construct a group G of twice the order of H by adding operators of order 4 which transform each operator of H into its inverse and have a common square. If H is cyclic and not of order 2, it is easy to find four such operators, each of which is a product of the other three. The smallest of these groups is the quaternion, and the four operators j, k, $-j$, $-k$ clearly satisfy the conditions

$$j\,.\,k\,.\,-j=-k,\quad k\,.\,-j\,.\,-k=j,\quad -j\,.\,-k\,.\,j=k,\quad -k\,.\,j\,.\,k=-j.$$

When H is the direct product of two cyclic groups, G may be constructed by dimidiation just as in the preceding paragraph; and if s_1', s_2' and s_1'', s_2'' are the generators of order 4 of the constituent groups, G may clearly be generated by $s_1' s_1''$, $s_1' s_2''$, $s_2' s_2^{-1''}$, $s_2^{-1'} s_1''$ and these satisfy the condition that each is the product of the other three in cyclic order. The results of this and the preceding paragraph exhaust the possible groups when H is Abelian and includes s_1^2. That is, if the order of s_1 is 2 or 4 and if s_1, s_2, s_3, s_4 are such that the product of any three, in a given cyclic order, is the fourth, then they generate one of the groups considered in this and the preceding paragraph whenever s_1^2 is in H. If s_1^2 is not in the Abelian H, s_1 is necessarily of order 4 and it is necessary to extend H by means of an operator (s_1^2) of order 2 which is commutative with all its operators. The remaining operators of G transform each operator of this extended H into its inverse and have a common square. Moreover, every such extended H will give rise to one G which is generated by four operators of order 4 satisfying the

* Cayley, Quarterly Journal of Mathematics, vol. 25 (1890), p. 71.

conditions imposed on s_1, s_2, s_3, s_4. Hence when H is Abelian G may be obtained by extending an Abelian group which has at most three invariants (if its maximal invariants are chosen) by means of an operator which transforms each operator of this Abelian group into its inverse.

It remains to consider the groups when H is non-Abelian. It has been proved that such an H is metabelian, contains a cyclic commutator subgroup, is invariant under G, and that the order of G is either twice or four times that of H. Moreover, the two generators of H $(s_1 s_2^{-1}, s_2 s_3^{-1})$ are independent of the commutator subgroup of H. That is, neither of these operators generates any commutator besides the identity, since such commutators are generated by s_1^4, and s_1^2 is invariant under G while s_2 transforms both $s_1 s_2^{-1}$ and $s_2 s_3^{-1}$ into their inverses. The orders of $s_1 s_2^{-1}$ and $s_2 s_3^{-1}$ are divisible by the order of s_1^4, and each of the operators s_1, s_2, s_3, s_4 is of even order. The last statement follows from the fact that if s_2 were of odd order it would be commutative with s_2, s_3, s_4, since they have the same square. Hence it would also be commutative with $s_1 s_2^{-1}$, $s_2 s_3^{-1}$ and the orders of these operators could not exceed 2. These operators would therefore be commutative, since s_1^4 could not be of order 2. This proves the theorem: *If the n operators $s_1, s_2, \ldots, s_n$ are arranged cyclically and the product of any $n-1$, in order, is the remaining one, then all are of even order when $n < 5$.*

From the preceding paragraph it follows that H may be constructed by extending the direct product of two cyclic groups, which are such that the order of the one is a divisor of the order of the other, by means of an operator which is commutative with the generator of one of these groups and transforms the generator of the other into the product of the two generators. It follows that the order of the extending operator is also divisible by the order of the invariant generator. Moreover, any such group can be used for H, since the two generating operators in question may be replaced by s_1^4 and $s_1 s_2^{-1}$, and the extending operator may be replaced by $s_2 s_3^{-1}$. It is then possible to find an operator which has the properties imposed on s_2, since it is possible to establish a simple isomorphism of H with itself in which s_1^4 corresponds to itself and each of the operators $s_1 s_2^{-1}$, $s_2 s_3^{-1}$ corresponds to its inverse. The last statement follows from the fact that $s_3 s_2^{-1}$ transforms $s_2 s_1^{-1}$ into $s_1^4 \cdot s_2 s_1^{-1}$ and $s_2 s_3^{-1}$ transforms $s_1 s_2^{-1}$ into $s_1^4 \cdot s_1 s_2^{-1}$. As the quotient group G/H is cyclic and of order 2 or 4, it is easy to construct all the possible G's for any particular H. It may be observed that the properties of all of these groups are somewhat similar to those of the dihedral type. In particular, all of them are solvable.